Solicitors Regulation Authority

Information and cyber security

23 November 2020

'Cybercrime continues to rise in scale and complexity, affecting essential services, businesses and private individuals alike. Cybercrime costs the UK billions of pounds, causes untold damage, and threatens national security.' National Crime Agency, 2019

'Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19.' Jürgen Stock, INTERPOL Secretary General1 [#n1]

Why this risk matters

Law firms hold critically sensitive information and large sums of money for people and businesses.

In the first half of 2020, firms told us that nearly £2.5m of money held by firms had been stolen by cybercriminals, over three times the amount reported in the first half of 2019. Much of this was covered by insurance but the losses also mean people experience stress and delayed or prevented transactions.

The lockdowns have made firms more dependent than ever on technology. Many firms needed to adjust in a hurry. This means that some systems are more vulnerable to attack. And, the threats have grown. For example, there was a 337% rise in phishing scams in the first two months of the first national lockdown.2 [#n2]

Ransomware is becoming more serious. It is not always possible to recover affected data, even after paying the ransom. As well as denying access to files, it increasingly copies the information and threatens to release it. Firms should now assume that a ransomware attack has breached confidentiality of the information they hold.

Additional costs of cyberattacks to firms include:

- higher insurance premiums
- having to pay for financial losses
- lost time
- damage to client relationships
- lost jobs
- stress and pressure on staff.

For example, one firm lost around £150,000 worth of billable hours after an attack.3 [#n3] While not all attacks succeed, the scale of the threat and impact is clear.

Our thematic review [https://www.sra.org.uk/sra/how-we-work/archive/reports/cyber-security/] found that the cost of mitigating cyber threats is usually much lower than the losses of a successful attack. Protecting your firm and people's data and money, therefore, makes business sense, as well as being a regulatory requirement.

Who is most at risk?

Any firm holding money or confidential information is a potential target.

Staff who have not received cybercrime training are at the highest risk. Most cybercrimes target people, usually by 'phishing', which tricks someone into opening a false attachment or clicking on a fake link. This could allow the criminals to steal password information, read or forward confidential emails, or install malware. If not detected, they might have access for a considerable time. This is more likely where a system has not been updated.

Staff who work from home might be at increased risk of cyberattacks and confidentiality breaches. For example, because:

- home wifi and the use of staff's own devices might be less secure than the office network or work-issued devices
- those without dedicated office spaces or secure document storage might find it hard to keep information confidential from those they live with and visitors
- staff are less likely to know who is in the office or online, which can make cyberattacks, such as CEO fraud, easier.

Those using video meetings, including virtual courts, need to use them carefully and securely. For example, make sure that unauthorised parties cannot overhear or see a confidential meeting or materials.

While social media can be a useful tool for marketing and communication, it can be a source of risk. Criminals can use information gained from media posts to learn more about a firm for phishing.

We recommend

Know your obligations

All firms should:

- Know the requirements of the Code of Conduct and Accounts Rules about people's money and information.
- Have procedures for dealing with cyber risks.
- Know when you need to report incidents to us, to the Information Commissioner's Office (ICO), and to law enforcement. For example:
  - Certain cybercrime incidents involving personal data need to be reported to the ICO within 72 hours.
  - Any cybercrime that has accessed people's emails has breached personal data.
  - Any missing client money is a breach of our Accounts Rules.
  - You need to report successful attacks even if you or your insurer have already repaid any financial losses.
- Know when and how to engage with your insurer(s).

'…the need for everyone to remain cybercrime vigilant has never been higher. Law firms should make sure that they have effective cyber security policies in place, and, crucially, that everyone in the firm understands and follows these day to day'. Paul Philip, Chief Executive, SRA4 [#n4]

Have the right controls

Ask yourself	Actions to help you control the risk
Do you regularly review and update your risk assessment on how you might be exposed to cybercrime?	You can arrange an independent assessment and certification of your risks, such as Cyber Essentials Plus [https://www.ncsc.gov.uk/cyberessentials/overview] , and make sure that you keep that certification up to date. You can test your processes and assessments to check for vulnerabilities.
Are you confident that you have effective policies and procedures to protect information and money?	You could consider whether alternatives such as third-party-managed accounts (TPMAs) might improve your ability to protect people's money.

Do you have a plan for what to do, and how to recover, if your firm has a major cyberattack?	If your pre-Covid-19 response plans were based on all staff being in the office, you need to update them if most staff are now homeworking. You need to make sure that your plan is in a safe place and available offline.
Does your insurance cover the potential costs of a successful cybercrime?	Some firms have a cyber budget as a contingency fund and for investing in suitable cyber security. If you have diverted funds to deal with Covid-19, you should check whether you are protected against a cyberattack.
Have all your staff had relevant training on cybercrime and information security, particularly on how to recognise phishing attempts?	You can better protect data and money if you know the transactions and data that criminals might exploit. Everyone needs to remain vigilant for email modification fraud attempts and not rely on Confirmation of Payee. This fraud is a common threat, where criminals forge an email saying that bank details have changed. You can help people to protect themselves by telling them about this threat and having a process in place for this situation. Everyone should know the common signs of potential phishing attempts [https://www.ncsc.gov.uk/guidance/suspicious-email-actions] . You and your staff also need to know how to keep devices secure, for example, by creating effective passwords and avoiding unsafe devices, such as datasticks, where possible.
Has your firm got a ‘no blame’ culture?	Making sure that staff feel able to report incidents promptly will allow you to take defensive steps to protect against losses.

If you use cloud systems, are you confident that they are secure?	It is important to look at the accreditation of potential cloud suppliers. You should understand what you are responsible for, such as making sure the privacy settings are appropriate.
Do you keep your IT systems up to date and replace software that is no longer supported?	Updates often fix known issues, but out of date software might not receive them.
Do you have multiple secure backups of your data?	Having more than one secure backup of your data will help you to recover after an attack.

Get more information

Our cyber security Q&A [https://www.sra.org.uk/sra/news/cyber-security-qa/] has information about how to minimise the risks of homeworking and remote meetings.

The National Cyber Security Centre (NCSC [https://www.ncsc.gov.uk/]) has advice and guidance for firms of all sizes. This includes:

- Guidance on remote working [https://www.ncsc.gov.uk/guidance/home-working] , video meetings [https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations] and specific advice for smaller firms [https://www.ncsc.gov.uk/smallbusiness] .
- Guidance for businesses considering a ‘bring your own device’ [https://www.ncsc.gov.uk/collection/mobile-device-guidance/bring-your-own-device] approach, and on how to safely use cloud services. [https://www.ncsc.gov.uk/collection/cloud-security]
- Advice on recognising and dealing with phishing scams. [https://www.ncsc.gov.uk/guidance/suspicious-email-actions]
- Advice on policies around the use of passwords [https://www.ncsc.gov.uk/collection/passwords/updating-your-approach] and other security systems.

- Free online elearning on defending against cybercrime and a free exercise [https://www.ncsc.gov.uk/information/exercise-in-a-box] to help firms test their resilience.
- Advice about new threats, such as criminal attacks on some cloud-based systems. [https://www.ncsc.gov.uk/news/rise-microsoft-office-365-compromise]

The British Standards Institution has advice about homeworking [https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2020/march/expert-advice-on-remote-working-from-bsis-cyber-security-and-information-resilience-team/] .

Cyber Essentials Plus [https://www.ncsc.gov.uk/cyberessentials/overview] is a government-supported scheme. It helps you assess your cyber security and has an external certifying body that audits your systems. Being certified under Cyber Essentials entitles some firms [https://iasme.co.uk/cyber-essentials/cyber-liability-insurance/] to cyber liability insurance and technical help.

The ICO has guidance on your requirements under the General Data Protection Regulation (GDPR) and advice on how to protect you and consumers. And they have guidance on data protection and the coronavirus.

The Law Society's advice on cyber security for solicitors [https://communities.lawsociety.org.uk/practical-support-features/cybersecurity-when-working-from-home/6000880.article?utm_source=professional_update&utm_medium=email&utm_campaign=PU-03%2f27%2f2020] discusses how to protect your systems and comply with the GDPR.

Case example: Firm affected by phishing attack

The senior partner in a firm received an email that appeared to be from a client but was a phishing attack. When they clicked on an attachment, it automatically sent emails to the partner's existing contacts which asked them to click on a link and give information.

As soon as the firm realised what had happened, they:

- asked their bank to freeze their client account
- called their IT suppliers for advice
- self-reported to us
- said sorry to affected clients
- investigated to find out about any harm and to prevent any future attacks.

The firm found that no client money or confidential information had been affected. We took no further action because the firm had taken

quick and proactive action following the human error and had prevented any losses.

Case example: Long lasting attack on solicitor's email account

One solicitor noticed that emails were arriving out of time order and with a delay. They told their IT provider, who found that unauthorised rules were applied to the solicitor's email account about a month before. These rules forwarded all messages with the word 'purchase' to the criminals, giving them targets for email modification fraud. This happened because the solicitor had responded to a phishing message.

The firm:

- self-reported to us and to the ICO
- secured their IT systems, including getting help from specialists and changing all passwords
- contacted their clients to tell them about email modification fraud and telephoned those with pending transactions.

We took no further action against the firm but gave them advice on further steps they should take to protect consumers and prevent further attacks.

What we are doing

Helping firms and solicitors

Our Risk Outlook and our report on technology and legal services [https://www.sra.org.uk/archive/risk/risk-resources/technology-legal-services/] includes advice from the NCSC on how to secure information against cybercrime. And we have advice on how to protect information [https://www.sra.org.uk/sra/news/cyber-security-qa/] while staff are working from home.

We support innovations that improve firms' ability to protect consumers' money and data. For example, our reforms have made it easier for firms to use TPMAs which can reduce their exposure to cybercrimes that target your customers' money.

Our recent thematic review of cybercrime [https://www.sra.org.uk/sra/how-we-work/archive/reports/cyber-security/] helped us to understand how firms and the public are affected by cybercrimes. We are working with other regulators to continue to build our understanding of the risks from cybercrime.

Taking appropriate action

When we receive reports about cybercrimes, we take a proportionate view. We know that mistakes can happen. We will look at whether the firm had reasonable protective measures in place and how they remedied the situation, where appropriate.

On the horizon

INTERPOL report that:

- cybercrime is likely to carry on increasing because the economic downturn and working from home can make many businesses vulnerable
- when Covid-19 vaccines and treatments are released, phishing attacks about these are likely to spike.5 [#n5]

The Law Commission is consulting [https://www.lawcom.gov.uk/project/reform-of-the-communications-offences/] on proposals to improve the legal protection for victims of harmful online behaviour. Their consultation ends on 18 December 2020.

In future, more types of business will use distributed ledger technologies, or blockchains, for example, for smart contracts. The Law Society has advice for firms [https://www.lawsociety.org.uk/en/topics/research/blockchain-legal-and-regulatory-guidance-report] on what to look out for when using these systems.

Notes

1. INTERPOL, INTERPOL report shows alarming rate of cyberattacks during COVID-19 [https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19] , 2020
2. NCSC, Weekly Threat Report 21st August 2020 [https://www.ncsc.gov.uk/report/weekly-threat-report-21st-august-2020] , 2020
3. SRA, Thematic review of cybercrime [https://www.sra.org.uk/sra/how-we-work/archive/reports/cyber-security/] , 2020
4. SRA, Greater than ever need for law firms to remain cybersecure [https://www.sra.org.uk/sra/news/press/2020-press-release-archive/cybercrime-thematic-review/] , 2020
5. INTERPOL, INTERPOL report shows alarming rate of cyberattacks during COVID-19 [https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19] , 2020